IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEIZURE OF 1 DOMAIN NAME CONTROLLED BY PUBLIC INTERNET REGISTRY 1) garantex.org	Case No. 1:25-sw-177
IN THE MATTER OF THE SEIZURE OF 2 DOMAIN NAMES CONTROLLED BY IDENTITY DIGITAL 1) garantex.academy 2) garantex.io	Case No. 1:25-sw-178 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT

I, Special Agent Ryan Schmidt, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since in or around March 2017. I am currently assigned to the Cyber Investigative Section, Criminal Investigative Division, in Washington, DC. Upon entering the USSS, I completed 18 weeks of basic training. This training covered various aspects of federal law enforcement, including instruction on the investigation of financial crime. I have investigated numerous individuals for a wide variety of federal and state felony offenses, including computer fraud and access device fraud. Furthermore, I have attended more than 160 hours of USSS training pertaining to computer investigations involving cyber and electronic crimes.

2. The facts and information contained in this Affidavit are based upon my personal knowledge of the investigation, observations of other law enforcement officers and agents involved in this investigation, and information provided by known sources of information. All observations referenced below that I did not personally make were related to me by the persons who made such observations. Moreover, this Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on the facts as set forth in this Affidavit, I submit that there is probable cause to believe that the property set forth in the "Assets to be Seized" section of this affidavit are involved in violations of 18 U.S.C. § 1956(h), Conspiracy to Commit Money Laundering, and are subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1). I make this affidavit for a warrant to seize the property described in Attachments A-1 to A-3, specifically the **SUBJECT DOMAIN NAMES.** The procedure by which the government will seize the Domain Names is described in Attachments A-1 to A-3 hereto and below.

ASSETS TO BE SEIZED

4. I make this affidavit in support of an application for a seizure warrant for the following domain names:

- garantex.org ("**SUBJECT DOMAIN NAME 1**")
- garantex.academy ("**SUBJECT DOMAIN NAME 2**")
- garantex.io ("**SUBJECT DOMAIN NAME 3**")

(collectively, the "**SUBJECT DOMAIN NAMES**"). **SUBJECT DOMAIN NAME 1** is controlled by Public Internet Registry, a top-level authoritative domain registry headquartered at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston VA 20190. **SUBJECT DOMAIN NAMES**

2 and 3 are controlled by Identity Digital, a top-level authoritative domain registry, which has its headquarters at 10500 NE 8th Street, Ste. 750, Bellevue, WA 98004.

LEGAL AUTHORITY

5. 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) prohibits, in pertinent part, whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such financial transaction which in fact involves the proceeds of specified unlawful activity knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

6. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. § 1701, *et seq.*, granted the President the authority to deal with unusual and extraordinary foreign threats to the national security, foreign policy, or economy of the United States. Under IEEPA, the President can declare a national emergency and issue Executive Orders that have the full force and effect of law. Among other things, IEEPA empowers the President to impose economic sanctions on a foreign country. It is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to IEEPA. 50 U.S.C. § 1705(a). Pursuant to 18 U.S.C. § 1956(c)(7)(D), the term "specified unlawful activity" includes violations of IEEPA. Pursuant to IEEPA, the President issued Executive Order 14024 on April 15, 2021, finding that specified harmful foreign activities of the Russian government, including engaging in and facilitating malicious cyber-enabled activities against the United States and its allies and partners, constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. Executive Order 14024 provides that all property and interests in property in the United States or within the

possession or control of any U.S. person of any person designated pursuant to this Executive Order must be blocked (i.e., frozen) and may not be transferred, paid, exported, withdrawn, or otherwise dealt in. It also prohibits (a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any such designated person; (b) the receipt of any contribution or provision of funds, goods, or services from any such person; and (c) any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order.[1]

7. Pursuant to 18 U.S.C. §§ 982(a)(1) and 981(a)(1)(A), any property, real or personal, which was involved in a violation of 18 U.S.C. § 1956, is subject to criminal and civil forfeiture. Moreover, any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of that same offense is subject to forfeiture pursuant to 18 U.S.C. § 982(a)(1) and 18 U.S.C. § 981(a)(1)(C).

8. Title 18, United States Code, Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found. Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts giving rise to the forfeiture occurred, even as to property located outside the district.

9. Title 18, United States Code, Section 982(b)(1) authorizes the issuance of a

[1] As discussed further below, on or about April 5, 2022, OFAC designated Garantex pursuant to this Executive Order. *See* OFAC Press Release, Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex, Apr. 5, 2022, https://home.treasury.gov/news/press-releases/jy0701.

criminal seizure warrant under Title 21, United States Code, Section 853(f), which provides in relevant part that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order may be inadequate to assure the availability of the property for forfeiture.

10. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SUBJECT DOMAIN NAMES** for forfeiture. By seizing the **SUBJECT DOMAIN NAMES** and redirecting them to another website, the Government will prevent third parties from acquiring the names and using them to commit additional crimes. Furthermore, seizure of the **SUBJECT DOMAIN NAMES** will prevent third parties from continuing to access the **SUBJECT DOMAIN NAMES** in their present form.

11. Title 18, United States Code, Section 981(h) provides that venue for civil forfeitures brought under this section lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought. Section 981(h) applies only in cases of property of a defendant charged with a violation that is the basis for the forfeiture of the property. Otherwise, under section 981(h), venue is determined under Title 28, United States Code, Section 1395. Section 1395 provides that a civil forfeiture action may be maintained in the district where the offense giving rise to forfeiture was committed, the district where the subject property is found, or any district into which the property is brought.

12. Title 21, United States Code, Section 853(l), which is made applicable to criminal forfeiture under Title 18, United States Code, Section 982(b)(1), provides that U.S. district courts shall have jurisdiction to enter orders without regard to the location of any property which may be

subject to forfeiture. Venue for criminal forfeitures lies in the district where the criminal prosecution may be brought.

DEFINITIONS

13. **Digital Currency:** Digital currency (also known as cryptocurrency, or virtual currency) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currency is legal in the United States and accepted for legitimate financial transactions. However, it is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership or control of illegally obtained proceeds. Some of the most common digital currencies include Bitcoin (BTC), Ether (ETH), Tron (TRX), and Tether (USDT).

14. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDC is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

15. **Tether:** One type of the most common types of tokens is Tether (USDT), a token issued by Tether Limited. Tether Limited is the company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens. USDT tokens can be hosted on the Ethereum or Tron networks. USDT is a "stablecoin" whose value is pegged to the U.S. dollar; allegedly all USDT tokens are completely backed by U.S. dollar reserves under the ownership or control of Tether Limited.

16. **Blockchain:** Many digital currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by

the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every digital currency address that has ever received that digital currency and maintains records of every transaction and all the known balances for each digital currency address. There are different blockchains for different types of digital currencies. For example, BTC, ETH, and TRX each operate on their own respective blockchain networks – Bitcoin, Ethereum, and Tron.

17. **Digital Currency Exchange:** A digital currency exchange is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick-and-mortar and online exchanges accept a wide variety of digital currencies and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. The types of exchanges can vary from large, established, and licensed businesses that operate under and follow strict know-your-customer (KYC) and Anti-Money Laundering (AML) policies to unlicensed individuals operating without adherence to U.S. federal regulations governing virtual currency exchanges. Exchanges operating within the United States are required to be registered with the Financial Crimes Enforcement Network (FinCEN), an arm of the U.S. Department of the Treasury, and as such, are required to follow certain money transmitter regulations and KYC/AML regulations. Individuals involved in criminal activity often prefer to use unregulated and unlicensed exchanges to purchase digital currency with unlawful proceeds or cash out Bitcoin acquired through illegal activity, because these exchanges do not typically request and store the type of information required under KYC and AML guidelines.

18. **Cryptocurrency Address:** A cryptocurrency address is identified by a unique electronic address that essentially stores the access code that allows an individual to conduct transactions on the public ledger. To access an address on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are described as "pseudonymous," meaning they are partially anonymous.

19. **Cryptocurrency Wallet:** Multiple cryptocurrency addresses controlled by the same individuals are referred to as a wallet.

20. **Blockchain Analysis:** As previously stated, while the identity of a digital currency address owner is generally anonymous, law enforcement can identify the owner of a particular digital currency address by analyzing the blockchain or when the address owner uses certain digital currency exchanges. The analysis can also reveal additional addresses controlled by the same individual or entity, referred to as "clusters." In addition to using publicly available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies, to investigate digital currency transactions. These companies analyze digital currency blockchains and attempt to identify the individuals or groups involved in transactions. Many of these companies create large databases that group cryptocurrency addresses into "clusters" through analysis of data underlying Bitcoin transactions. A cluster is an estimate of all

the cryptocurrency addresses contained in a user's cryptocurrency wallet or wallets. This type of blockchain analysis software is frequently used by financial institutions, including legitimate cryptocurrency exchanges, to detect and prevent money laundering and other criminal activity, as well as by law enforcement organizations worldwide, because these tools provide subscribers with warnings about wallets associated with criminal activities including fraud, ransomware, and dark markets, among others.

21. **Internet Protocol Address ("IP Address"):** A unique numeric address used by computers on the Internet. A version-4 IP Address ("IPv4") is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

22. **Domain Name:** A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., "justice.gov"). Domain names are composed of one or more parts, or "labels," delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the "top-level domain" ("TLD") (e.g., ".com" or ".gov"). To the left of the TLD is the "second-level domain" ("SLD"), which is often thought of as the "name" of the domain. The SLD may be preceded by a "third-level domain," or "subdomain," which often provides additional information about various functions of a server or delimits areas under the same domain. For

example, in "www.justice.gov," the TLD is ".gov," the SLD is "justice," and the subdomain is "www," which indicates that the domain points to a web server.

23. **Domain Name System ("DNS"):** The Domain Name System ("DNS") is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

24. **Domain Name Servers:** Domain Name Servers ("DNS servers") are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS "clients." For example, the registry servers for the ".org" top-level domain is controlled by Public Internet Registry.

25. **Registrar:** A company that has been accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") or a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

26. **Registrant:** The person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically "point" their domain name to the IP address of the server where the registrant's website is hosted.

27. **Registry:** A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the

public. For each top-level domain (such as ".org"), there is a single company, called a "registry" that determines which second-level domain resolves to which IP address.

PROBABLE CAUSE

28. Since approximately in or around April 2021, USSS has been investigating Garantex, a Russian-operated cryptocurrency exchange that is currently the subject of sanctions issued by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). Garantex is routinely used to both facilitate and launder the proceeds of criminal activity including ransomware,[2] computer hacking by state actors, use of darknet markets,[3] as well as terrorism financing. The administrators of Garantex are aware that Garantex is used for these purposes, actively seek to avoid preventing such activity, and profit from such activity. To that end, Garantex fails to conduct basic KYC/AML checks on its customers, thus providing a means for criminal organizations to launder illicit funds. When Garantex does identify criminal activity on its platform, it fails to take prompt remedial measures and instead continues to allow its platform to be used for criminal ends. Additionally, Garantex has deliberately restructured its business operations to evade, and cause violations of, U.S. sanctions and to render it more difficult for law enforcement—as well as financial institutions and other third parties obligated to comply with

[2] "Ransomware" is a type of malicious software program that encrypts contents of a victim computer or computer network and removes the ability for a victim to access its computer or computer network. In order for the victim to regain access to the computer or computer network, the victim must pay a ransom, typically in bitcoin, to the attackers in exchange for receiving the required decryption keys.

[3] Darknet markets are platforms used by criminals to buy and sell illicit goods such as drugs. They may also provide additional services to facilitate criminal activity, including serving as a payment intermediary or escrow agent for a criminal transaction. For example, if someone were to buy drugs using a darknet market, they could either transact directly with the drug dealer, or they could send the money to the forum administrator, who would ensure that the buyer receives the drugs before the dealer is paid.

OFAC and FinCEN regulations—to detect and block transactions with Garantex. Garantex also operates as an unlicensed money service business in the United States.

29. Garantex is thus designed and intended to facilitate criminal transactions and conduct and to launder the proceeds. As discussed below, basic Internet searches, cryptocurrency analysis, undercover transactions, and evidence obtained from copies of Garantex's customer and administrator databases indicate that the **SUBJECT DOMAIN NAMES** are used in furtherance of these schemes. As such, there is probable cause to believe the **SUBJECT DOMAIN NAMES** are subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).

I. Background on Garantex and SUBJECT DOMAIN NAMES

30. Garantex was founded in or around 2019 and operated primarily from its website hosted at garantex.io, while also maintaining accounts on social media platforms such as Telegram. Garantex advertised the ability to carry out transactions for conversions of cryptocurrency to cryptocurrency, cryptocurrency to fiat currency, and fiat currency to cryptocurrency. Funds could be exchanged in the fiat currencies of Russian Rubles, U.S. Dollars, and Ukrainian Hryvnia. Cryptocurrencies that could be exchanged included BTC, USDT, ETH, and several others. Garantex claimed that customers could withdraw funds at offices in Moscow and Saint Petersburg, Russia, as well as a network of partner offices across Russia, Ukraine, and around the world. Garantex, according to its website, claimed to take a fee of approximately 0.1% to 0.2% of each transaction, depending on the nature of the transaction.

31. In or around February 2022, Garantex lost its license to provide digital currency services after Estonia's financial regulatory authority revealed critical anti-money laundering deficiencies and found connections between Garantex and digital currency wallets used for

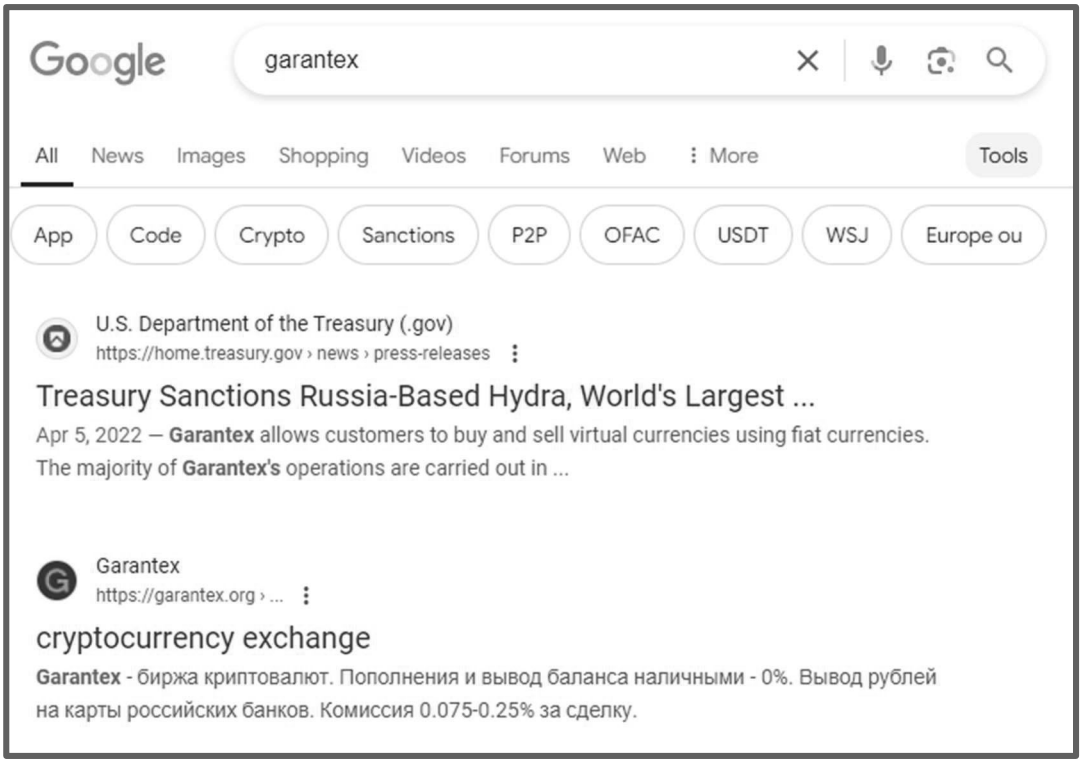
criminal activity. Nonetheless, Garantex continued to offer services without meaningfully improving its anti-money laundering practices.

32. On or about April 5, 2022, OFAC sanctioned Garantex.[4] The OFAC press release noted that the majority of Garantex's operations was carried out in Russia, including at Moscow-based Federation Tower, where other sanctioned digital currency exchanges have also operated. OFAC's analysis of known Garantex transactions (using reliable blockchain analysis tools) showed that over $100 million in transactions were associated with illicit actors and darknet markets, including nearly $6 million from the Russian ransomware actors behind Conti ransomware, and approximately $2.6 million from Hydra, a Russia-based darknet market.[5] OFAC's press release thus further put Garantex on notice of the fact that it had been used for assorted criminal activity and that it was subject to U.S. sanctions.

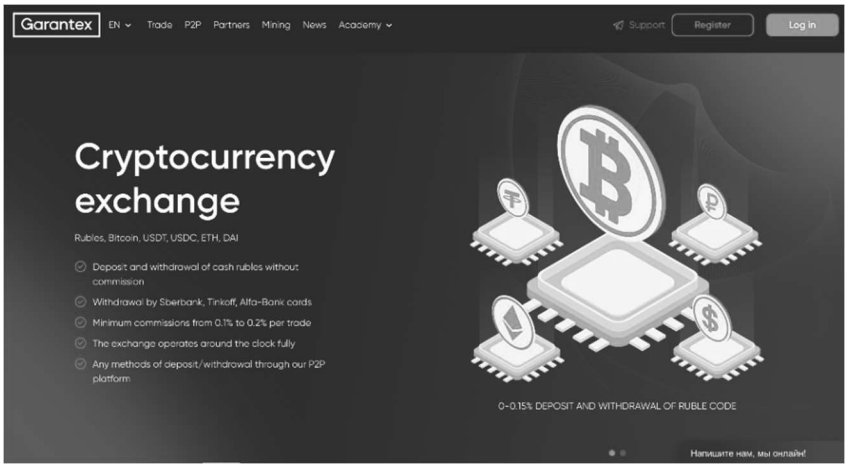
33. Today, Garantex primarily operates from websites hosted at **SUBJECT DOMAIN NAME 1** and **SUBJECT DOMAIN NAME 2**, which are accessible to the general public, to include U.S.-based persons. **SUBJECT DOMAIN NAME 1** is the primary website operated by Garantex and used by Garantex customers to access the exchange's services. Internet searches conducted via the Google search engine in or around September 2024 for keyword "garantex" show that **SUBJECT DOMAIN NAME 1** is listed second in search results, just after the OFAC press release announcing sanctions. Thus, anyone with Internet connectivity can easily search for and access Garantex via **SUBJECT DOMAIN NAME 1**, as demonstrated in the following screenshot:

[4] https://home.treasury.gov/news/press-releases/jy0701.

[5] At the time of sanctions, Garantex had facilitated an overall volume of at least $2.4 billion in transactions of bitcoin *alone* since its launch in 2019.



34. The webpage hosted at **SUBJECT DOMAIN NAME 1** allows interested parties to register with Garantex, sign into an existing account, or contact Garantex's support team for assistance. The page also provides information on the specific exchange rates charged by Garantex for the purchase or sale of specific cryptocurrencies, instructions on how to download Garantex's mobile application, general information concerning different products offered by Garantex, and similar items. Below is a screenshot of the webpage captured by USSS on or about February 14, 2025 (machine translated from Russian):



35. On **SUBJECT DOMAIN NAME 1,** Garantex has published a terms of service that claims that Garantex "does not provide services to residents and citizens of the United States" and that customers were not permitted to make or participate in transactions on the Garantex platform or use any of Garantex's services if the user was a resident or citizen of the United States or if, per the website, "the User is included in the Specially Designated Nationals And Blocked Persons List by the U.S. Office of Foreign Assets Control, or in the Denied Persons List by U.S. Department of Commerce." Garantex does not follow or enforce these terms of service.

36. **SUBJECT DOMAIN NAME 2** functions as an education resource offered by Garantex. On **SUBJECT DOMAIN NAME 2**, Garantex provides a variety of tutorials and learning materials concerning general cryptocurrency trading and similar investing topics, but also specific courses on how to utilize Garantex. For example, up to at least in or around February 2025, the main webpage for **SUBJECT DOMAIN NAME 2** offered a free beginner's course that included a 60-minute web tutorial on accessing and navigating the Garantex website and learning about trading options, including how Garantex compares with other exchanges in terms of functionality. The following is a screenshot of Russian-language text captured in or around September 2024 from **SUBJECT DOMAIN NAME 2** advertising this specific course:

37. The above text translates roughly to the following:

> *Functionality of the Garantex exchange*
> *Duration: 60 minutes*
> *In this webinar, we will discuss in detail the capabilities of the Garantex exchange. We will study the functionality of the exchange, consider all available operations, and tell you which button is responsible for what.*

38. In other words, **SUBJECT DOMAIN NAME 2** supports the operations of **SUBJECT DOMAIN NAME 1** by providing the necessary learning resources to interested parties on how to navigate the various exchange services advertised on **SUBJECT DOMAIN NAME 1**.

39. **SUBJECT DOMAIN NAME 3** functioned as Garantex's primary website before the platform shifted to **SUBJECT DOMAIN NAME 1** in late 2023. In other words, **SUBJECT DOMAIN NAME 3** was previously the main mechanism used by Garantex customers to access the exchange's services. Although Garantex no longer operates its website from **SUBJECT**

DOMAIN NAME 3, domain registration records show that the domain remains active and that its registration is valid until on or about November 1, 2025.[6]

II. Overview of Garantex's Facilitation of Illicit Activity and Money Laundering

40. As described in further detail below, Garantex has been integral to facilitating and concealing a variety of criminal activity being investigated and prosecuted by the Department of Justice including ransomware, funds stolen by hacking, and terrorism financing. The following paragraphs provide an overview of how Garantex is used to commit, conceal, and promote the aforementioned crimes.

A. Ransomware

41. Consistent with OFAC's April 5, 2022, press release, law enforcement and third-party firms have observed that Garantex has received significant volumes of funds originating from ransomware victims. Indeed, the press release announcing sanctions on Garantex described how $6 million of funds were funneled through Garantex from the Russian ransomware actors behind Conti ransomware.[7]

42. Pursuant to an unrelated USSS investigation into Conti ransomware, law enforcement conducted a forensic review of a server utilized by the Conti ransomware group to facilitate ransomware attacks. This review determined that one particular non-U.S.-based ransomware victim was directed to make payment to Bitcoin address

[6] Based on my training and experience, I know that, in the event law enforcement seizes a domain belonging to a criminal platform, the administrators of these criminal platforms will frequently shift to another domain under their control to allow the platform to remain operational. Given that **SUBJECT DOMAIN NAME 3** is still controlled by Garantex, the domain has been included in this seizure warrant to inhibit the ability of Garantex to quickly shift operations to this domain following the seizure of **SUBJECT DOMAIN NAME 1**.

[7] https://home.treasury.gov/news/press-releases/jy0701.

bc1qnf273myysxjw23g9hze4vcu3uqkget9ra70hen in exchange for regaining access to their systems. On or about June 30, 2021, the victim received a decryptor[8] from the attackers. A review of the Bitcoin blockchain revealed that on this same day, the aforementioned Bitcoin address received an approximate $430,000 payment. Approximately $170,000 thereof was subsequently transferred to Garantex.

43. As a further example, a major insurance provider confirmed that one particular U.S.-based victim attacked with Conti ransomware had made a payment of approximately $311,220 to Bitcoin address bc1qyu6v00l89ytfyl459kd6ehjrhjdxacz3f8qhsx on or about June 26, 2021. Approximately $166,000 thereafter was subsequently transferred to Garantex.

44. Based on my training and experience, I know that ransomware actors will transfer funds from their own wallets, through intermediate wallets, to professional money laundering services or exchanges that do not respond to law enforcement requests and do not follow anti-money laundering best practices in order to launder illicit proceeds, pay other actors involved in the ransomware attacks, and to conceal the control and ownership of the funds.

45. Likewise, a February 2022 blog post by Chainalysis, a reliable cryptocurrency forensics company utilized by numerous law enforcement agencies, observed that Garantex had received at least $10 million from ransomware strains Netwalker, Phoenix, CryptoLocker, and Conti from 2019 to 2021.[9] The imposition of sanctions on Garantex has not changed these patterns: since the imposition of sanctions, law enforcement has identified numerous additional instances

[8] In the context of ransomware, a "decryptor" is a piece of software provided by an attacker to a victim so that the victim can regain access to their encrypted systems. Ransomware attackers will typically only provide a decryptor to a victim after the victim makes a ransom payment.

[9] https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/

of ransomware funds being laundered through Garantex. For example, law enforcement has an ongoing investigation into an active ransomware group ("Ransomware Group 1") that launched in or around June 2022 and has been responsible for attacks on approximately 300 different organizations globally, including organizations in the United States. Using blockchain analysis tools, this investigation has determined that, between in or around November 2022 and in or around April 2024, approximately BTC 481/$16.7 million in victim funds (approximately 80 percent comprised of U.S. victims) originating from attacks associated with Ransomware Group 1 were ultimately deposited to Garantex.[10]

46. In addition, the investigation into Ransomware Group 1 has determined that the group relies primarily on a Russia-based third-party money launderer ("Launderer 1") to process funds originating from victims of Ransomware Group 1. Indeed, investigation has revealed that Launderer 1 launders funds for other ransomware groups.

47. The investigation determined that Launderer 1 maintains at least two accounts at another digital currency exchange ("DCE 4"). Records obtained from DCE 4 demonstrate the following concerning those two accounts:

a. DCE 4 Account 1: Between in or around June 2020, and in or around June 2023, this account received approximately $115 million in USDT on Tron from various sources, to include Ransomware Group 1. Over the same time period, the account sent approximately $164,000 in USDT on Tron to Garantex.

[10] Because of the sanctions placed on Garantex, its alleged laundering of funds from Hydra and other criminal marketplaces, and widespread media reporting throughout 2023 and 2024 on Garantex's involvement in facilitating illegal monetary transfers for a host of other criminal organizations, Garantex cannot be relied upon to cooperate with law enforcement or furnish customer records in good faith. As a result, law enforcement has been unable to fully investigate transactions associated with groups such as Ransomware Group 1.

b. DCE 4 Account 2: Between in or around June 2023, and in or around December 2023, this account received approximately $16.8 million in USDT on Tron from various sources, to include Ransomware Group 1. Over the same time period, the account sent approximately $329,000 in USDT on Tron to Garantex.

48. A study from in or around November 2023 also noted that Garantex had received approximately $10 million in payments from victims of the Black Basta ransomware group since early 2022.[11]

49. Furthermore, a reliable blockchain analytics tool indicates that Garantex's overall incoming transaction volume has an "indirect exposure" to ransomware payments and ransomware groups amounting to at least BTC 849 (approximately $71 million based on the current exchange rate) between in or around February 2018 and in or around June 2024, through a total of approximately 600,000 incoming transfers. The concept of "indirect exposure" in this case refers to a measurement of deposits that ultimately originate from ransomware, but were not made directly from a ransomware address to a Garantex address and instead involved multiple intermediary addresses before the funds in question were deposited to Garantex. This type of calculation is typically more reliable in terms of quantifying overall ransomware deposits handled by Garantex than simply reviewing direct exposure, as ransomware organizations will usually not receive victim funds and transfer those funds directly to an exchange like Garantex. Instead, ransomware payments will usually first flow through several intermediary addresses for various

[11] The original study can be found at https://www.elliptic.co/blog/black-basta-ransomware-victims-have-paid-over-100-million. Although the report focuses on a $100 million overall figure allegedly generated by Black Basta, USSS held a separate conversation with Elliptic and determined the specific amount transferred to Garantex was approximately $10 million.

reasons, to include concealment techniques employed by the ransomware organization or simply due to the specific Bitcoin wallet software utilized by the organization, among other reasons.

50. Consistent with the above analysis, a review of indirect payments between ransomware organizations and Garantex revealed multiple instances of Garantex handling ransomware deposits, including as recently as last year. For example, on or about February 8, 2024, Garantex received an approximate $226,000 deposit that originated from a wallet utilized by the Black Basta ransomware group to receive an approximately $1 million ransom payment from a U.S. victim (consistent with the pattern identified by the study described above).

B. Network Intrusions

51. In or around June 2022, hackers stole $105 million worth of digital currency from a U.S.-based blockchain network through a network intrusion. Law enforcement determined that after the funds were stolen, the attackers used a sophisticated series of transfers to launder the funds, but that at least $22 million were transferred to a digital currency exchange ("DCE 2"), which cooperates with law enforcement. Information furnished by DCE 2 confirmed that the account receiving the $22 million was registered to email address proforg@gmail.com and registered with the identifiers Aleksej BESCIOKOV, a known Garantex administrator, who USSS had separately tied to the technical infrastructure operation of Garantex.

52. Furthermore, USSS determined that the email account proforg@gmail.com and the DCE 2 account registered to Administrator A have been used to support the overall operations of Garantex, including after sanctions were imposed on it.[12] As a result, there is probable cause to

[12] For example, in or around December 2022, USSS served a search warrant for the contents of proforg@gmail.com, which yielded numerous artifacts associated with the operation of Garantex, to include files that appeared to be development or back-up versions of Garantex's customer and administrator databases. The transaction activity of the DCE 2 account registered to Administrator A also revealed multiple incoming USDT transfers originating from Garantex.

believe that Garantex is involved in facilitating funds transfers resulting from network intrusions conducted by hacker groups.

C. Terrorism Financing

53. In or around March 2024, Israel's National Bureau for Counter Terror Financing of Israel (NBCTF) issued Administrative Seizure Order 5/24 (ASO 5/24 or the "Order") in which it listed 42 digital currency addresses that it had determined were the "property of a designated terrorist organization, or property used for the perpetuation of a severe terror crime."[13] The NBCTF determined that the addresses in question were used primarily to facilitate transactions on the Tron network. The Order also listed a group of specific individuals who were associated with these transfers and who maintained accounts at a major digital currency exchange ("DCE 3") that responds to law enforcement requests. A separate NBCTF publication[14] provided the transaction history of these terrorism-related accounts at DCE 3, listing three specific addresses, among others, as having been direct transactional counterparties and therefore also associated with terrorism.

54. USSS reviewed the transaction activity of these three addresses and, utilizing the copies of Garantex servers that contain customer and transaction databases that USSS had obtained via search warrants in the Eastern District of Virginia, determined that each of the three terrorism-associated addresses had made direct USDT transfers to specific accounts at Garantex on multiple occasions in or around January, May, June, September, and October of 2022.

55. As described further below, USSS also obtained copies of Garantex's server infrastructure, which yielded information on the processes, or lack thereof, the exchange used to screen customer transactions for illicit activity. Copies of Garantex server infrastructure obtained

[13] https://nbctf.mod.gov.il/he/Announcements/Documents/%D7%A6%D7%AA%205-24.pdf

[14] https://nbctf.mod.gov.il/en/Minister%20Sanctions/PropertyPerceptions/Pages/Blockchain1.aspx

by USSS, described further below, indicate that Garantex utilized one particular commercial provider of blockchain analytics software ("Software Company A") to monitor transactions on the Garantex platform. Garantex began using Software Company A on or about March 29, 2019, but did not start flagging transactions for "terrorism_financing," a specific category of monitoring offered by Software Company A, until on or about April 1, 2022, just before Garantex was sanctioned. Software Company A terminated its relationship with Garantex on or about April 6, 2022, following the imposition of sanctions, and Garantex did not resume using any monitoring software until in or around June 2023. Then, between on or about June 13, 2023, and on or about November 23, 2023, another blockchain analytics software company ("Software Company B") utilized by Garantex flagged 20 deposits into Garantex as "terrorism_financing," and the status of those deposits in the Garantex database is listed as "accepted." Based on my training and experience, I believe that the notation "accepted" means the particular transaction was processed.

D. Other Illicit Activity[15]

56. As noted in the previously referenced April 2022 OFAC press release, OFAC's analysis of known Garantex transactions (using reliable blockchain analysis tools) showed that, up until that point, over $100 million in transactions processed by Garantex were associated with illicit actors and darknet markets, including approximately $2.6 million from Hydra, a Russia-based darknet market.

57. USSS similarly performed blockchain analysis to review known Garantex transactions, both pre- and post-sanctions, and determined that Garantex has processed large volumes of digital currency funds to and from multiple additional illicit sources, thus further

[15] As discussed in additional detail in later sections, Garantex has also facilitated and laundered proceeds from sanctions violations.

indicating that Garantex fails to combat money laundering conducted on its platform. A non-exhaustive list of examples of funds from darknet marketplaces or other criminal sources that Garantex has processed include the following:

a. In or around July 2020 to in or around April 2023: approximately $2,570,000 from Exploit, a Russian-speaking online criminal forum utilized by a variety of elite cybercriminals.[16]

b. In or around March 2021 to in or around October 2023: approximately $634,000 from and $380,000 to Blacksprut, a Russian darknet market that specializes in drug sales.

c. In or around March 2022: approximately $380 from a known child abuse website.

d. In or around December 2022 to in or around December 2023: $24,000 from and $155,000 to Kraken Market, a darknet market that specializes in drug sales.

e. In or around September 2023: approximately $280,000 from PM2BTC, a long-time professional Russian money laundering service advertised primarily on cybercrime forums and designated by FinCEN on or about September 26, 2024, as an entity of "primary money laundering concern" in connection with Russian illicit finance.

58. Indeed, compared to most compliant exchanges with meaningful KYC/AML programs, Garantex allows disproportionately higher volumes of illicit transactions on its platform, thus further indicating that Garantex actively encourages the facilitation of funds transfers on behalf of multiple kinds of cybercrime organizations and services. For example, a 2023 annual

[16] Online criminal "forums" are typically platforms that function as message boards, allowing members to discuss various topics, exchange idea and tips, and collaborate on committing crimes.

report published by Chainalysis[17] noted that in one particular 60-day period prior to OFAC sanctioning Garantex on or about April 5, 2022, 6.1% of incoming funds deposited to Garantex originated from illicit sources, with an additional 16.1% of incoming deposits originating from sources categorized by Chainalysis as "risky."[18] According to Chainalysis, these percentages are significantly higher than legitimate, law-abiding centralized exchanges, with the latter as a whole receiving, on average, approximately 0.3% of incoming deposits originating from illicit activities during that same 60-day period—meaning Garantex had *twenty times* more incoming deposits from illicit sources as a percentage of its overall deposits than legitimate exchanges. Notably, Chainalysis also observed that from 2019 to 2021, 31% of all of deposits to Garantex was from illicit or risky sources.[19]

59. Furthermore, law enforcement has identified multiple examples of members of online criminal forums recommending Garantex as a reliable platform to launder funds, thus indicating that the exchange was generally known to facilitate transfers associated with illicit activities. For example, in response to a discussion topic on high quality cryptocurrency exchangers posted on one Russian-speaking forum, a forum member noted on or about November 23, 2022, that Garantex was a convenient platform to exchange cryptocurrency to a Tinkoff code and then to use the code to withdraw cash from a Tinkoff Automated Teller Machine (ATM) while

[17] https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/

[18] According to the Chainalysis annual report, "[r]isky activity refers to transactions in which one or more counterparty addresses are associated with a risky entity, such as a high-risk exchange or gambling service. Legitimate activity refers to transactions in which one or more counterparty addresses are associated with entities that are not inherently criminal or risky, such as personal wallets or exchanges."

[19] https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/

wearing a covid mask, presumably to hide one's facial identity from ATM cameras. Tinkoff is a Russian financial institution that is also currently the subject of OFAC sanctions. Based on my training and experience, the reference to a Tinkoff "code" corresponds to a Tinkoff Quick Response (QR) code, which functions similar to a barcode, and allows Tinkoff customers to transfer funds to one another using QR codes.

60. Similarly, in response to another discussion topic, a forum member suggested on or about July 10, 2023, that one would need contacts in the Russian Federal Security Service (FSB) or Garantex in order to safely launder large amounts of funds from a hack.

III. Garantex's Awareness of Illegal Activity on its Platform

61. There is probable cause to believe that the Garantex administrators know that it is being used to launder a significant volume of funds from illicit and risky sources and continues to provide services to those criminal actors. Among other things, Garantex was sanctioned by the United States in or around April 2022 for facilitating illicit activity, putting it on notice that such activity was taking place on its platform. The other public reporting on Garantex discussed above also would have put it on notice about the criminal activity on its platform. Finally, it used monitoring software to track high-risk transactions on its platform but nevertheless permitted twenty times more deposits from illicit sources as a percentage of overall deposits than legitimate exchanges.

62. Based on my training and experience, I know that legitimate cryptocurrency exchanges attempt to implement robust AML and KYC programs on their platforms to combat illicit activities, such as money laundering or terrorism financing, and to ensure that they are complying with local laws and regulations in the jurisdictions in which they operate. As a result, legitimate exchanges have relatively low volumes and percentages of illicit activity occurring on

their platforms, as noted above. The Garantex administrators, however, have failed to implement such programs—despite having the tools to do so—and as a result, Garantex has both a high volume and percentage of illicit activity on the platform.

63. Garantex's administrators' lax KYC/AML approach is corroborated by materials obtained by USSS from Garantex's server infrastructure provider.[20] Specifically, USSS secured multiple search warrants in the Eastern District of Virginia for server infrastructure at a U.S.-based server infrastructure provider utilized by Garantex to store copies of its primary Bitcoin wallets and customer databases, among other components of its business. USSS executed its first such search warrant in or around September 2021. USSS also executed multiple search warrants in the period following the imposition of sanctions.[21] In response to these search warrants, USSS obtained copies of Garantex's customer database, as well as copies of accounts operated by the administrators of Garantex. Among other things, this data shows that Garantex's administrators were actively aware that certain customers were engaged in criminal behavior, but nonetheless continued to provide services to those criminal customers. The following is a non-exhaustive list of examples:

[20] A "server" is a computer that provides services to other computers. Examples include web servers which provide content to web browsers and email servers which act as a post office to send and receive email messages. In the context of cryptocurrency exchanges like Garantex, servers can provide various functions, to include providing interfaces allowing customers to create accounts and trade on its platform, as well as servers that host Bitcoin wallets utilized by Garantex to facilitate customer transactions.

[21] Based on my training and experience, I am aware that certain server infrastructure providers maintain servers worldwide and may store customer data in geographical jurisdictions that are different from the geographic location of the actual servers leased by a specific customer of interest, and that the customers may not be aware of this fact. In this context of Garantex, the last search warrant return received by USSS was in or around November 2023. At this time, the U.S.-based server infrastructure provider largely hosted backup copies of Garantex's server configuration that Garantex had leased in a foreign country.

a. An account registered to username "Crypto_slava" actively engaged in transactions on Garantex from in or around February 2021 until in or around late 2023, despite having been flagged by Garantex administrators on or about August 4, 2022, as involved in the laundering of cryptocurrency. Although they implemented a temporary block on the account, that block was removed less than one month later on or about September 9, 2022, and the user was able to continue trading through at least 2023 (when the USSS's access to data ends[22]).

b. Administrator notes indicate that Garantex user "uirist," one of the highest volume accounts on the platform, was warned on or about September 20, 2023, to stop transferring funds originating from ransomware. However, despite the warning, Garantex administrators permitted the account to continue transacting up until at least on or about November 14, 2023, at which point the USSS's access to data ended.

c. Administrator notes dated in or around October 2022 indicate that, in response to an inquiry to an account registered to username "Juicy_Fruit," the accountholder admitted that its account was possibly involved in a transaction for a client of Juicy_Fruit that constituted laundering funds related to narcotics trafficking. Despite this admission, Garantex administrators permitted Juicy_Fruit to continue trading on the Garantex platform through at least in or around November 2023 (and possibly longer), noting that the account was likely a money "exchanger." USSS separately obtained a copy of a server in the Netherlands that Juicy_Fruit had rented

[22] USSS secured another copy of Garantex's servers in May 2024, but has not finished analyzing that data.

and determined through analysis of the seized forensic data, such as Random Access Memory (RAM) dumps,[23] that the user was providing a service to assist narcotics traffickers with establishing an online presence (*i.e.*, establishing a website, .onion domain[24], and a Telegram bot[25]), in addition to providing cryptocurrency exchange services. In my training and experience, law-abiding exchanges would not have permitted a user such as Juicy_Fruit to continue using their services after linking the account to narcotics trafficking and money exchanging.

d. Administrator notes from 2023 for an account registered to "global.crypto44@proton.me" include numerous entries about possible dirty funds and other problems, including a note reading, "blocked, Terrorism Financing 100%!!!" This note was apparently later reversed with a note reading "everything's ok." However, data from Software Company B for the account show that it was engaged in high-risk activities, despite the administrator comments noting otherwise.

[23] RAM is short-term memory storage utilized by a computer or computer system to fulfill various tasks more efficiently.

[24] A .onion domain is a website that is only accessible using specific software and is hosted on what is called the "Tor" network, which provides anonymous web browsing services, among other things.

[25] Telegram is a popular Russia-based social media platform that provides a variety of services, to include encrypted communications platform, online marketplaces, and commercial advertising, among others. Individual users or entities can register Telegram "accounts." Individuals and entities can also create Telegram "channels," allows users to broadcast messages, communications, advertising, etc. to a large number of subscribers to said channels. Telegram "bots" are accounts or channels that are programmatically designed to automatically answer certain questions and are popular with various online service providers to handle customer queries without the need for a human to perform these tasks.

e. An account registered to alice.spam@yandex.ru was opened on or about October 6, 2023, and transacted only around that time. An administrator note reads, "eth, btc from Terrorism Financing," although there is a subsequent note that it is from a charitable organization. Another note indicates that the account was referred to compliance. The account does not appear to have been verified.

64. Furthermore, copies of Garantex's customer database revealed multiple accounts that were clearly fictitious or dubious in nature, but which had been allowed by Garantex administrators to continue using the exchange. For example, a search of the Garantex customer database revealed the following registered users, among many others: "Drug," "hacker," "taliban," "Cashout," "cleancoins," and "God." While other accounts did contain apparently more complete or accurate information, any efforts to obtain such information were not consistent or uniform. Based on my training and experience, as well as Garantex's informal, haphazard, and frequently non-existent approach to even the most basic KYC/AML practices, it appears the Garantex administrators were at least willfully blind to and more likely actively accepting of the use of its platform for illicit purposes.

65. As previously noted, seized Garantex infrastructure indicated that Garantex failed to flag terrorism-related transactions up until on or about April 1, 2022. Similarly, Garantex administrators also did not start flagging for transactions related to child sexual abuse material or international sanctions, categorized in Software Company A's tool as "child_exploitation" and "sanctions," respectively, until on or about April 1, 2022. Garantex did not utilize any other provider to flag transactions. In other words, in contrast to most law-abiding exchanges, despite launching in approximately 2019, Garantex had no known mechanism to screen for transactions involving child exploitation, sanctions, or terrorism-related transactions up until on or about April

1, 2022, despite having received approximately 394,000 incoming deposits totaling $2.4 billion in bitcoin alone between on or about December 31, 2019, and on or about March 31, 2022.

66. Moreover, according to USSS's review of the Garantex database, Garantex ceased using Software Company A on or about April 6, 2022, and did not appear to use any other transaction monitoring firm until on or about June 3, 2023, when it started using Software Company B. Starting on or about November 7, 2023, Garantex again switched providers and began to use a third software company to flag transactions by risk.

67. Even in the periods when Garantex did use tools to monitor and flag transactions, USSS's review of the Garantex database shows that administrators did not block many transactions identified by Garantex's software as "high risk." Representatives of Software Company A confirmed that while Garantex was using its services, Garantex had access to a feature that provided Garantex with a risk scoring framework to automatically flag transactions as associated with illegal or risky activities. Software Company A further advised that the product's risk scoring feature could be self-customized to allow clients such as Garantex to tailor the tool according to the AML/KYC requirements for different regions or countries in which they operate, for example. Based on my training and experience, in addition to having reviewed seized copies of another crypto exchange that used Software Company A, I understand that the risk score for any given transaction ranges from 0 to 1.000, with 1.000 being the highest. Between on or about May 16, 2019, and on or about April 6, 2022, approximately 15,000 incoming deposits to Garantex were flagged as having a risk score of 1.000, the highest possible risk score. Of those transactions with the highest risk scores, only 247 (or 1.6%) were marked as "rejected," 7 were notated as "suspected," 11 were marked as "fraudulent," and all remaining approximately 15,000 were marked as "accepted." Moreover, even when specific transactions were rejected, accounts

receiving these transactions—including accounts believed to be receiving funds from ransomware—were allowed to continue transacting on Garantex.[26]

68. From in or around June 2023 to in or around March 2024, while Garantex was using Software Company B and another blockchain analytics company, Software Company C, it received approximately 219 notifications that a deposit was flagged as having a risk score of 1.000. Of these flagged transactions, no transactions were marked as "rejected"—all 219 deposits had a status of "accepted."

69. Over a dozen of these 219 deposits went to Garantex Account No. XXX1134. Garantex administrators had made several notes about this account receiving funds from questionable sources, yet the account was still permitted to remain active. For example, one administrator wrote on or about June 28, 2023: "With him there's an agreement that a couple of times a month he can send to us from Wasabi, prof knows (Bonqai) unblocked /white." Wasabi is a mixing service that has been publicly linked to money laundering,[27] and USSS believes that "Bonqai" is a reference to Roman Storozhkov, a Garantex administrator (discussed below).

70. Along those lines, a July 2024 report by TRM, another reliable third-party cryptocurrency tracing and analysis firm that works frequently with law enforcement,[28] concluded that Garantex was responsible for facilitating 82% of cryptocurrency transactions conducted by sanctioned entities (both U.S. and international) in 2023. Because sanctions are public, and because

[26] During the period when Garantex was not subscribing to an external blockchain analysis provider, its servers nonetheless contain some notations reading "dirt_wallet" and "highrisk," though no additional context is available.

[27] https://www.elliptic.co/blog/elliptic-identifies-likely-use-of-wasabi-wallet-service-to-launder-twitterhack-bitcoins

[28] https://www.trmlabs.com/comrades-in-crime-exploring-the-russian-speaking-illicit-crypto-ecosystem

Garantex was receiving blockchain analysis data from two different companies for seven months in 2023, it should have been relatively easy for Garantex to identify and eliminate, or at least minimize, such activity on its platforms. Based on my training and experience with reputable blockchain analytics firms, I understand that such firms would have easily enabled Garantex to prevent transactions with sanctioned entities. The high percentages of these types of transactions occurring on the Garantex platform indicate Garantex was choosing to allow this activity to continue on its platform.

71. In addition, review of Garantex records revealed that Garantex administrators appeared to willfully provide misleading responses to law enforcement inquiries. A review of the seized Garantex infrastructure revealed multiple inquiries to Garantex from Russian law enforcement requesting information about specific accountholders. In one instance, on or about November 13, 2023, a Garantex representative advised Russian law enforcement that customer records associated with a specific requested wallet address belonged to an individual who registered with max@cryptomax.ru, who operated as an exchanger, and whose identifying information was not on file. The Garantex representative therefore directed Russian law enforcement to email max@cryptomax.ru to inquire further. However, the U.S. investigation has revealed that, in reality, max@cryptomax.ru and the corresponding Garantex account actually belong to Aleksandr MIRA SERDA, a cofounder and one of the primary administrators of Garantex, that Garantex in fact had MIRA SERDA's identifying information on file and associated with the account in question, and that Garantex failed to disclose this information to Russian law enforcement—even while disclosing identifying information related to other accounts requested by Russian law enforcement.

IV. Garantex's Efforts to Avoid Transaction Monitoring and Cause Sanctions Violations

72. Since being sanctioned by OFAC, Garantex has implemented an operating wallet infrastructure that is designed to avoid having its transactions and operations blocked by other digital currency exchanges and to cause sanctions violations.

A. Garantex's Deliberate Changing of Operating Wallet Infrastructure for USDT Assets

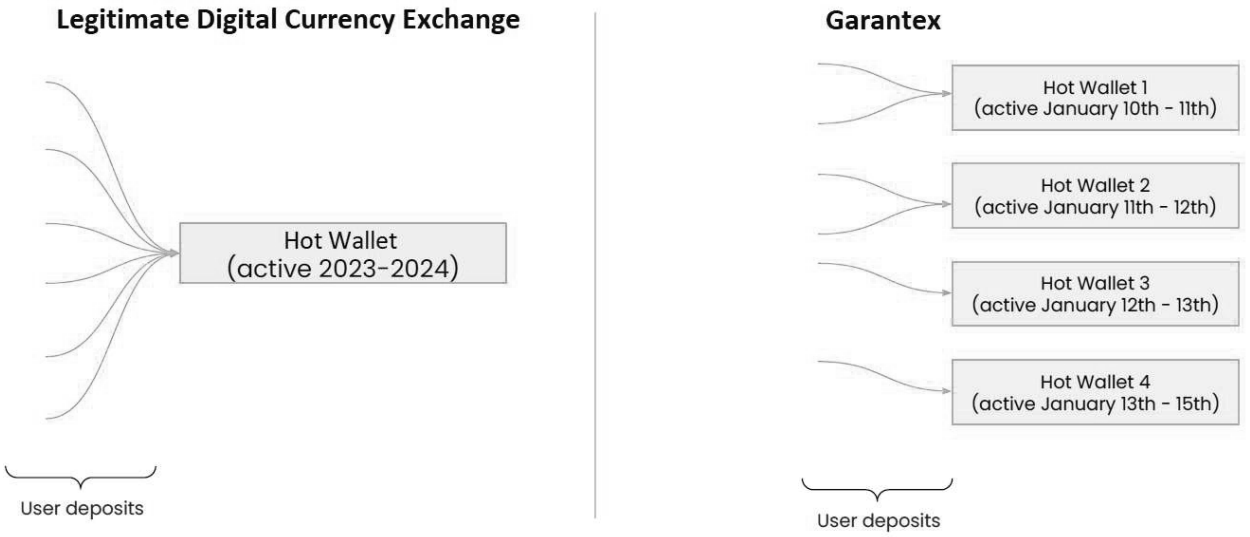
73. Research conducted by Elliptic, a reliable cryptocurrency analytics and research provider that works frequently with law enforcement, shows that, after U.S. sanctions were imposed on it, Garantex deliberately changed its business model and infrastructure practices to render it more difficult for financial institutions, such as other digital currency exchanges, to comply with U.S. sanctions by monitoring and blocking Garantex-performed transactions, as well as to render it more difficult for law enforcement to detect Garantex-performed transfers and seize Garantex-related funds. These changes ultimately have allowed Garantex to surreptitiously continue its participation in the financial and cryptocurrency ecosystems without fear of reprisal, isolation, detection, or disruption. Garantex implemented these changes across multiple different blockchain networks used to support currencies offered on its platform, to include USDT, which comprises the majority of Garantex's transaction volume at present, according to Elliptic.

74. The primary step taken by Garantex to counter third party transaction monitoring and blocking efforts involves changes to the platform's usage of operational wallets (also referred to as "hot wallets"). In the context of digital currency exchanges, operational wallets are exchange-operated wallets connected to the Internet that facilitate the overall customer transactions performed on the exchange platforms at any given time. For example, operational wallets will be used for processing customers' internal trades (*i.e.*, USDT in the operational wallet can be sent to

a customer seeking to exchange BTC for USDT), consolidating incoming customer deposits,[29] and providing a funding source for the processing of customer withdrawals outside of the exchange platforms. Operational wallets function similarly to master treasury accounts at traditional financial institutions. The identification of an exchange's operational infrastructure is one of the primary ways that blockchain analysis and AML compliance companies use to attribute transactions, addresses, and wallets to specific known exchanges such as Garantex.

75. Beginning in early 2023, Garantex sought to evade this standard tracing and detection function by changing its operational wallets, on average, on a daily basis. Based on my training and experience, as well as conversations with USSS personnel who specialize in cases involving cryptocurrency, this practice is inconsistent with that of any known legitimate digital currency exchange similar in size to Garantex and a departure from Garantex's practices before sanctions were imposed on it. Based on my training and experience, there is no legitimate business reason for Garantex to continually replace its USDT operational wallet infrastructure outside of an intent to render it more difficult for financial institutions, as well as law enforcement, to detect, monitor, block, or seize its transactions. The following is a visual depiction of operational wallet transactions at legitimate digital currency exchanges versus Garantex:

[29] Operational wallets generally do not receive customer deposits directly. Instead, customers will transfer deposits to other addresses operated by an exchange, and the exchange will then "sweep" those transactions into its centralized operational wallet from there.



76. Garantex's operational wallets are most active on the Tron network, with USDT comprising the vast majority—up to 99.1 %—of assets processed by these Tron operational wallets every day.

77. Despite Garantex's attempts to conceal its activities, Elliptic has nonetheless been able to identify Garantex's operational wallets. Elliptic initially began tracking Garantex's operational wallet generation process through a combination of blockchain analysis, open-source research, and direct interactions with the Garantex website. Specifically, similar to other blockchain analytics firms, Elliptic had identified Garantex's original operational wallets that had been used for prolonged periods, prior to Garantex implementing its daily replacement practices. After sanctions were imposed on it, Garantex began reducing the period of operational wallet usage from longer-term operational wallets, to weekly operational wallets, and then to daily operational wallets. Elliptic was able to follow this sequence of events by performing blockchain analysis and tracing fund movements.

B. Garantex Inducement of U.S. Parties to Violate Sanctions

78. U.S. persons and entities are required to comply with U.S. sanctions. According to a March 2024 notice,[30] "[n]on-U.S. persons [and entities] are also subject to certain OFAC prohibitions. For example, non-U.S. persons [and entities] are prohibited from causing or conspiring to cause U.S. persons [and entities] to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions." There is probable cause to believe that Garantex causes U.S. parties to violate sanctions in at least two ways. First, Garantex continues to process transactions involving U.S. persons, thereby providing unlawful services to U.S. persons. Second, Garantex causes sanctions violations by deliberately changing its operational wallet infrastructure so that otherwise compliant U.S. entities or exchanges are prevented from detecting that they are entering into transactions with Garantex.

79. For example, in or around May 2024 and in or around October 2024, a U.S.-based digital currency exchange ("DCE 1") furnished records to USSS reflecting multiple transfers between U.S.-based customers of DCE 1, including customers located in the Eastern District of Virginia, and what law enforcement knew from its investigation to be addresses associated with Garantex. At least 131 of these U.S.-linked transactions occurred from in or around April 2022 (when Garantex was sanctioned) to in or around March 2024.

80. Another major FinCEN-registered digital currency exchange ("DCE 5") has similarly transacted with Garantex since Garantex was sanctioned. Based on conversations with USSS personnel who have interacted directly with DCE 5 over multiple years, I know that DCE 5 has a relatively mature transaction compliance program, which attempts to block transactions with sanctioned entities. A review of transactions between DCE 5 and Garantex revealed that they have

[30] https://www.justice.gov/opa/media/1341411/dl?inline

engaged in over 4,950 transactions with one another involving USDT on the Tron network since OFAC sanctioned Garantex in or around April 2022. These 4,950 transactions amounted to approximately $39.3 million in USDT sent from DCE 5 to Garantex and approximately $37.9 million in USDT sent from Garantex to DCE 5 since sanctions were imposed.

81. Similarly, a review of transactions between DCE 5 and Garantex revealed that they have engaged in over 520 transactions with one another involving USDT on the Ethereum network since OFAC sanctioned Garantex. These 520 transactions amounted to approximately $3.9 million in USDT sent from DCE 5 to Garantex and approximately $2.1 million in USDT sent from Garantex to DCE 5 since the imposition of sanctions.

82. Based on my training and experience, I know that entities such as DCE 5 would typically have the ability to block a significant portion of transactions with a sanctioned entity and would comply with its legal obligation to do so. It is therefore likely that DCE 5 permitted these transactions because it did not realize it was transacting with Garantex.

C. Garantex Statements Concerning USDT and Sanctions Circumvention

83. According to records obtained by USSS, Garantex administrators have knowledge of OFAC's sanctions on the company. For example, in a communication on or about April 6, 2022—the day after OFAC sanctioned Garantex—a Garantex administrator requested servers from an international server provider explaining that the entity had been added to the "OFAC SDN" list. Notably, on or about April 8, 2022, just days after the imposition of sanctions, Garantex administrators sent a mass email specifically noting that OFAC had sanctioned Garantex but stating—in the subject line of the email—"Garantex is operating normally." On or about April 14,

2022, Garantex's Chief Marketing Officer, Evgenia Burova, participated in an interview posted to Garantex's YouTube channel discussing the imposition of sanctions.[31]

84. USSS identified a Telegram channel registered to username @garantex_chs with an administrator of username @eugyyb.[32] This account is operated by Burova. Another administrator in the @garantex_chs channel is username @Bonqai. The seized Garantex databases indicate that @Bonqai is the Telegram handle associated with the email account storozhkov@garantex.io, which is a designated Garantex administrator account and belongs to Roman Storozhkov. In other words, Telegram channel @garantex_chs and the account @Bonqai are operated by Garantex leadership. A review of the contents and broadcasted messages of this channel revealed a public posting by @Bonqai dated on or about December 10, 2023, which noted, in Russian, the following:

> *"Tether only blocks wallets included in the OFAC list, currently there is only 1 wallet on this list, used by Garantex before April 2022 with a balance of 0, not a single Garantex wallet used after April 2022 is on the list […] Adding wallets to this list is a slow bureaucratic process that lags significantly behind Garantex's current business processes […] We closely monitor the global situation and constantly improve our work so that our clients can work peacefully […] Blocking wallets without significant legal grounds is a critical threat to Tether's reputation and business, so the list of blocked wallets will expand slowly and with a long delay."*

The above posting indicates that the Garantex leadership actively monitors the actions of OFAC and other authorities to create an environment in which its Tether/USDT infrastructure remains undetected so that its customers can transact and trade on its platform without interference. The posting also indicates that the administrators of Garantex believe that if they do not use the same wallet addresses on a recurring basis, OFAC will be unable to sanction their addresses or block

[31] https://www.youtube.com/watch?v=Y68iFDD0ADY.

[32] Telegram channel administrators are listed publicly in that channel.

transactions. In other words, this posting helps confirm that Garantex's daily wallet changes are in fact designed to make it more difficult for other institutions and the U.S. government to detect and prevent its transactions.

D. Public Reporting Suggests that Garantex Has a Broader Role in Helping Russian Businesses Circumvent U.S. Sanctions

85. In addition to causing sanctions violations by unknowing parties, public reporting suggests that Garantex offers a means by which Russian businesses intentionally evade U.S. sanctions. For example, in a Wall Street Journal article dated on or about April 1, 2024, a Russian arms smuggler, Andrey Zverev, boasted about evading sanctions restricting arms sales, explained that he would do so by using Tether, and stated that his preferred trading platform for using Tether was Garantex. In a blog post, Zverev explained that "'the evil regulators' in the U.S. and Europe wouldn't be able to shut Garantex down."

86. The Wall Street Journal article reported that a Garantex spokesperson denied that the exchange facilitates criminal activities but noted that Garantex "***appreciated Zverev 'giving a high appraisal of our services***.'" Based on my training and experience, I know that a corporate spokesperson for a legitimate business that is not interested in facilitating criminal activity would not welcome the endorsement of a known international arms dealer; instead, this statement is indicative of Garantex's intent to facilitate such activity. Indeed, according to the article, Garantex's founder, Sergey Mendeleev, had convened a meeting of crypto figures in or around April 2023 to discuss solutions to the challenges faced by Russian military importers impacted by U.S. sanctions.

V. Importance of SUBJECT DOMAIN NAMES to Garantex's Operations

87. Based on all of the aforementioned, there is probable cause to believe that Garantex functions as a money laundering operation, in the United States and abroad, and that Garantex

actively causes the violation of, and enables others to violate, U.S. sanctions. By extension, the **SUBJECT DOMAIN NAMES** allow, have allowed, or will allow Garantex to commit or cause others to commit money laundering and sanctions violations. Specifically, **SUBJECT DOMAIN NAME 1** allows customers anywhere in the world, to include in the United States, to access and transact on the Garantex platform. Similarly, **SUBJECT DOMAIN NAME 2**, which is operated by Garantex, provides interested parties anywhere in the world, to include in the United States, with specific instructions on how to navigate and trade on the Garantex exchange. **SUBJECT DOMAIN NAME 3**, which is still operated by Garantex, previously allowed customers anywhere in the world to access Garantex's platform.

88. A search of publicly available domain name registration records reveals the following about the **SUBJECT DOMAIN NAMES** used by Garantex:

a. Garantex.org was first registered on or about November 1, 2018, and is currently registered through on or about November 1, 2025. The registry operations for the .org top-level domain are managed by Public Internet Registry.

b. Garantex.academy was first registered on or about April 12, 2022, and is currently registered through on or about April 12, 2025. The registry operations for the .academy top-level domain are managed by Identity Digital.

c. Garantex.io was first registered on or about November 1, 2018, and is currently registered through on or about November 1, 2025. The registry operations for the .io top-level domain are managed by Identity Digital.

89. In or around February 2025, I visited the above domains, reviewed their content, and researched the domain registration details. The websites continue to function and allow customers to access the main Garantex exchange platform via **SUBJECT DOMAIN NAME 1**

and to access the Garantex learning repository via **SUBJECT DOMAIN NAME 2**. **SUBJECT DOMAIN NAME 3** does not currently host live webpages, but is actively registered and operated by Garantex; therefore, Garantex could relaunch a website on that domain at any given time.

SEIZURE PROCEDURE

90. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the .org top-level domain, Public Internet Registry, the registry for the .academy and .io top-level domains, Identity Digital, and the registry for the .net top-level domain, Verisign, shall be directed to restrain and lock the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with USSS or the Department of Justice.

91. In addition, upon seizure of the **SUBJECT DOMAIN NAMES** by USSS, Public Internet Registry, Identity Digital, and Verisign will be directed to associate the **SUBJECT DOMAIN NAMES** to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAMES** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

92. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are used in, have been used in, and/or intend to be used in facilitating and/or committing the SUBJECT OFFENSES. Accordingly, the **SUBJECT DOMAIN NAMES** are subject to forfeiture to the United States pursuant to 18 U.S.C. §§

981(a)(1)(A) and 982(a)(1) and I respectfully request that the Court issue a seizure warrant for the **SUBJECT DOMAIN NAMES**.

93. Because the warrant will be served on Public Internet Registry, Identity Digital, and Verisign, which control the **SUBJECT DOMAIN NAMES** and, thereafter, at a time convenient to them, will transfer control of the **SUBJECT DOMAIN NAMES** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

RYAN M SCHMIDT

Digitally signed by RYAN M SCHMIDT
Date: 2025.03.03 22:43:47 -05'00'

Special Agent Ryan Schmidt
United States Secret Service

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 4th day of March 4, 2025.

Honorable William B. Porter
United States Magistrate Judge

ATTACHMENT A-1

With respect to:

garantex.org

("**SUBJECT DOMAIN NAME 1**"), Public Internet Registry, which is the top-level authoritative domain registry for **SUBJECT DOMAIN NAME 1**, shall take the following actions to effectuate the seizure of **SUBJECT DOMAIN NAME 1**:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the United States Secret Service, by modifying the **SUBJECT DOMAIN NAME 1** authoritative DNS server entries to include the following:

   a. ns1.usssdomainseizure.com and ns2.usssdomainseizure.com,

   Or:

   b. Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to Public Internet Registry.

2. Prevent any further modification to, or transfer of, **SUBJECT DOMAIN NAME 1** pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAME 1** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAME 1** cannot be made absent court order or, if forfeited to the United States, without prior consultation with United States Secret Service.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAME 1** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"The domain for Garantex has been seized by the United States Secret Service pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Virginia. This investigation is being led by the United States Secret Service and the U.S. Attorney's Office for the Eastern District of Virginia, as well as the Federal Bureau of Investigation and the Criminal Division of the Department of Justice, and with the support of international partners at The Netherlands Police, Europol, the German Federal Criminal Police Office, and the Estonian National Criminal Police."

ATTACHMENT A-2

With respect to:

garantex.academy

("**SUBJECT DOMAIN NAME 2**"), Identity Digital, which is the top-level authoritative domain registry for **SUBJECT DOMAIN NAME 2**, shall take the following actions to effectuate the seizure of **SUBJECT DOMAIN NAME 2**:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the United States Secret Service, by modifying the **SUBJECT DOMAIN NAME 2** authoritative DNS server entries to include the following:

    a. ns1.usssdomainseizure.com and ns2.usssdomainseizure.com,

    Or:

    b. Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to Identity Digital.

2. Prevent any further modification to, or transfer of, **SUBJECT DOMAIN NAME 2** pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAME 2** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAME 2** cannot be made absent court order or, if forfeited to the United States, without prior consultation with United States Secret Service.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAME 2** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"The domain for Garantex has been seized by the United States Secret Service pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Virginia. This investigation is being led by the United States Secret Service and the U.S. Attorney's Office for the Eastern District of Virginia, as well as the Federal Bureau of Investigation and the Criminal Division of the Department of Justice, and with the support of international partners at The Netherlands Police, Europol, the German Federal Criminal Police Office, and the Estonian National Criminal Police."

ATTACHMENT A-3

With respect to:

garantex.io

("**SUBJECT DOMAIN NAME 3**"), Identity Digital, which is the top-level authoritative domain registry for **SUBJECT DOMAIN NAME 3**, shall take the following actions to effectuate the seizure of **SUBJECT DOMAIN NAME 3**:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the United States Secret Service, by modifying the **SUBJECT DOMAIN NAME 3** authoritative DNS server entries to include the following:

   a. ns1.usssdomainseizure.com and ns2.usssdomainseizure.com,

   Or:

   b. Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to Identity Digital.

2. Prevent any further modification to, or transfer of, **SUBJECT DOMAIN NAME 3** pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAME 3** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAME 3** cannot be made absent court order or, if forfeited to the United States, without prior consultation with United States Secret Service.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAME 3** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"The domain for Garantex has been seized by the United States Secret Service pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Virginia. This investigation is being led by the United States Secret Service and the U.S. Attorney's Office for the Eastern District of Virginia, as well as the Federal Bureau of Investigation and the Criminal Division of the Department of Justice, and with the support of international partners at The Netherlands Police, Europol, the German Federal Criminal Police Office, and the Estonian National Criminal Police."